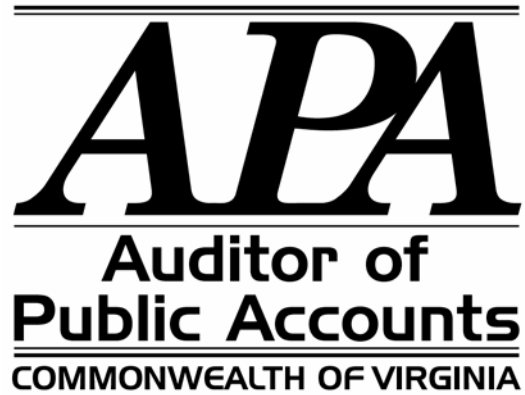
VIRGINIA EMPLOYMENT COMMISSION

RICHMOND, VIRGINIA

NETWORK VULNERABILITY ASSESSMENT AND PENETRATION TEST REPORT



AUDIT SUMMARY

Our network vulnerability assessment and penetration test of the Virginia Employment Commission (VEC) as of June 2004 found the following:

- Overall information security controls in place at the time of the testing appear sufficient to protect critical and sensitive information based on our assessment of the risks to the systems and our tests of the operating effectiveness of the controls developed by VEC to alleviate those risks; and

- VEC can make certain improvements to enhance systems security. We have provided management with the details of our findings and recommendations in a separate report exempted from public disclosure in accordance with Section 2.2-3705 (a) 45 of the Code of Virginia. This provision allows for the exemption from disclosure information that describes the design, function, operation, or access control features of any security system.

Commonwealth of Virginia

Walter J. Kucharski, Auditor

Auditor of Public Accounts
P.O. Box 1295
Richmond, Virginia 23218

June 2004

The Honorable Mark R. Warner
Governor of Virginia
State Capitol
Richmond, Virginia

The Honorable Lacey E. Putney
Chairman, Joint Legislative Audit
and Review Commission
General Assembly Building
Richmond, Virginia

The Virginia Employment Commission (VEC) requested the Auditor of Public Accounts (Auditor) to perform a vulnerability assessment and network penetration test. VEC requested that the Auditor use its technical staff experienced in security control work and operations to perform an independent assessment of the risks the systems face (vulnerability assessment) and a test of the operating effectiveness of the controls (penetration test). We conducted the review as of June 2004 and examined whether information systems management and administration had reasonably assessed risk and that the controls placed into operation were effective in mitigating the assessed risks.

VEC has created an information security controls environment that attempts to protect the areas where information systems management perceives risk and has tailored the controls accordingly.

The Auditors used a variety of scanning software and techniques during the vulnerability and penetration test. Outside of the scope of this engagement were "social engineering" attacks. Social engineering attacks include posing as technical support staff to elicit responses from users designed to aid in network penetration or searching desks to reveal notes with passwords and user IDs. This type of test typically identifies significant security weaknesses. However, we did not perform this type of test work because of the effect that these tests can have on employee confidentiality, property rights, and the relationship between users and information systems staff.

We limited this project to the VEC network. This test work did not include any information housed for VEC at the Virginia Information Technologies Agency (VITA). This engagement did not have a goal of identifying all of the potential weakness to which the systems could be subject.

Based on our assessment of the risks the systems face and the tests of the operating effectiveness of the controls developed by VEC to alleviate those risks, overall information security controls in place at the time of the testing appear sufficient to protect critical and sensitive information. However, we noted certain areas where management can make improvements to enhance systems security. We have provided management the details of our findings and recommendations in a separate report exempted from public disclosure in accordance with Section 2.2-3705 (a) 45 of the Code of Virginia. This provision allows for the exemption from disclosure information that describes the design, function, operation, or access control features of any security system.

We discussed this report with management at an exit conference held on October 22, 2004. We have not included management's response in this report because the information included in their response is also exempted from public disclosure in accordance with Section 2.2-3705 (a) 45 of the Code of Virginia. However, management concurred with our findings and agreed to take appropriate corrective action.

AUDITOR OF PUBLIC ACCOUNTS

KJS/kva